A REVIEW OF MOBILE BANKING INFORMATION SECURITY AND PROTECTION METHODS IN AFGHANISTAN

[1] Mohammad Fahim Naseri ,[2] Mr.Dushyant Sing
[1] Research scholar ,[2] Assistant Professor , Vivekananda Global University ,Jaipur , India
[1] Department of Computer Science & Engineering ,
[1] Vivekananda Global University ,Jaipur , India

Abstract: Through the help of up-to-date information communication technology, moveable (Mobil) banking as a new sort of business facilities importer can deliver effectual and effective economic services for clients. Relate with Internet banking, mobile banking is added security and user sociable. The employment of wireless communication technologies may result in more difficult information safety problems. Based on the principles of information security, this paper presented issues of information security of mobile banking and deliberated the security defence action such as: Encryption technology, individuality authentication, digital signature, WPKI technology. In result If banks can mix the mobile banking and present services, make good use of the welfares provided by of wireless communication technology such as cell phones and develop a single customer focused on services, mobile banking will be capable to play a more significant role in banking business.

Key words: Mobil banking, Data, Security, Encryption, technology

I. INTRODUCTION

II. After 2001 and the advent of mobile phones in Afghanistan, The country has been able to adapt to the world in the field of technology application, one of the most development area is new banking system With the wide-expansion of mobile telecommunication technology into the industry world, mobile banking converted the common and favourable banking technique in bank business recently. Mobile banking can provide clients with good worth and more cost-saving services. It mentions to provision and a ailment of banking and business services with the help of mobile communication devices. The space of provided services may include services to manner bank and asset market transactions, to manage accounts and to contact modified data. Most of the mobile banking researchers agreed that mobile banking contains of three parts: mobile accounting, mobile brokerage and mobile fiscal information services. For customer service sector including: balance checking, account transactions, payment, etc. conservative banking services. Progressively, bank clients will expect real-time information and access 24 hours a day, seven days a week, wherever they are in the world. Services such as electronic account management, mobile brokerage and monetary information and alerts enable banks and network workers to growth bank's modest edge and reinforce customer loyalty. Mobile banking can deliver perspective specific, location-based services (LBS) associated to banks. Compare with Internet banking, mobile banking is added security and more user friendly. Mobile banking not only can provide old-style bank services, but also proposal customer with 3A services (whenever, anywhere and anyhow). The suitable, effective and efficient mobile banking service has been the main reason to interest more customers. The security is the basis for mobile banking development. As mobile banking services multiply, the weak receivers and related platforms will become hacks or crooks attacking targets progressively. Some Mobile devices can present many of the same risks as Internet banking. In this paper discuses about some major security issue in banking information security in Afghanistan.

2. The Problems in Mobile Banking Information Security

2.1 The Process of Mobile Banking

A mobile banking system includes a mobile banking unit and a data processing core which may be the mainframe computer of the bank answerable for processing banking communications and data storage. The mobile banking contains one or more banking stations such as ATMs, deposit machines and hypermedia question stations. Mobile banking system has delivered a good basis for providing adapted, client- oriented, new model of business services, which includes a number of wireless communication channels, mix the qualities of different technologies the following （fig.1） shows the Mobile banking prosecco

.

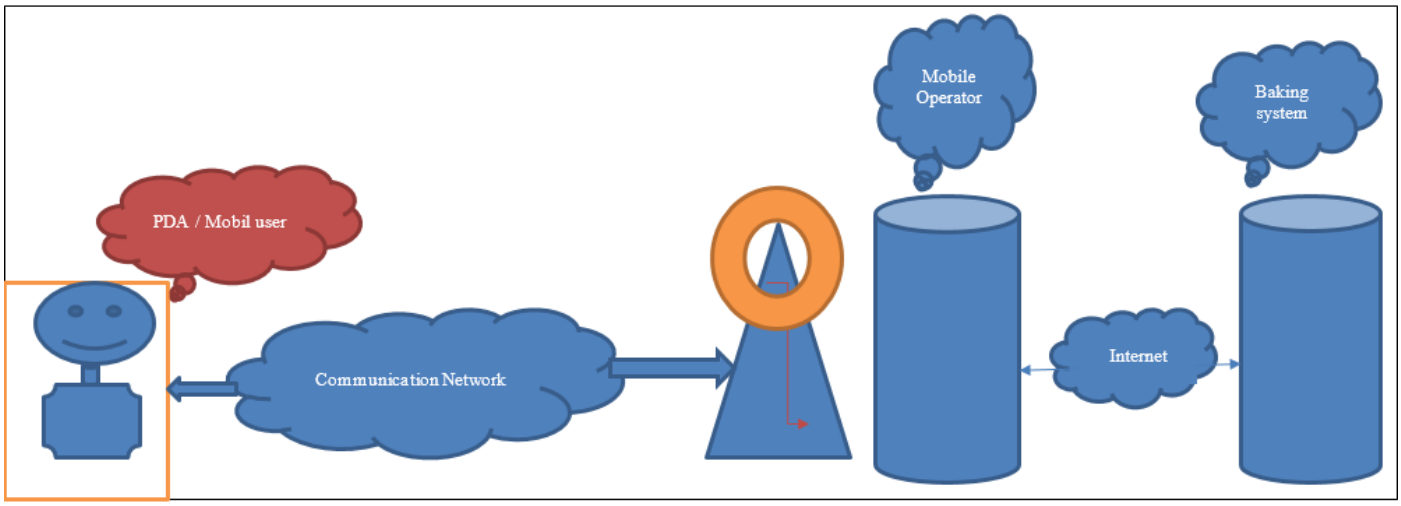

Figure 1 Mobile banking process

The properties of network business services have been the mark of all kinds of technology crimes since it arisen. Mobile banking has two security zones the below figure shows these zone

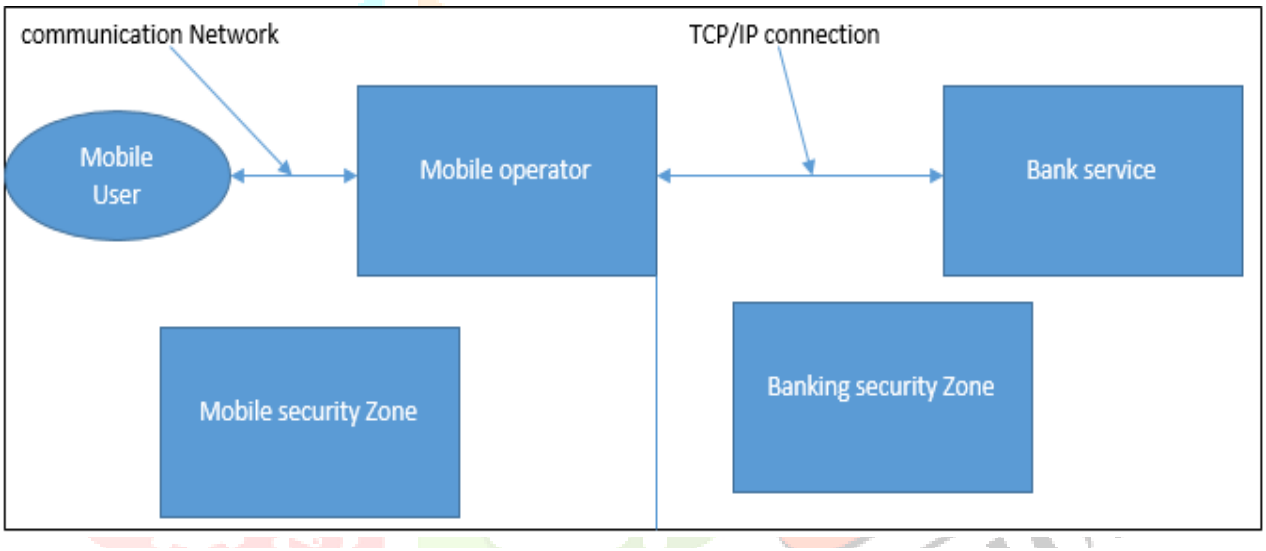

Figure 1 security zone in Mobile banking

Indicator set users' zone and mobile worker zone; Mobile operatives and bank system areas. The info security glitches in network banking such as hackers, virus attacks, etc. will be happened in mobile banking system operation as well. And specially In Afghanistan, there are the following problems in mobile banking.

2.2 The software run by the user

Afghanistan is one of the poorest countries in the Asia and the literacy rate in the country is reported to be around 60%. according to the ministry of education of Afghanistan. For the same reason, most Afghan citizens use the cracked Application and attack also depends on the application which is used by users. as we know Afghanistan is a country which 80 % of population is installs some cracked applications on digital devices like (smart phono, computers, etc.) these applications is not secure and also they are can not provide securely connection, these Application might be provide backdoor to unauthorized user the cyber-crime can assay attack on these type of application, this is one of the most issue in mobile banking system in Afghanistan.

2.2.1 Information leakage loss and distort

Mobile banking operation transmissions information done by wireless network. Wireless data networks need radios that take in digital data, zeros—and ones, moderate and transfer the data as radio waves, get the radio waves, demodulate the signal, and change them back to zeros and ones. Existence is the capacity to have many radios operating without nosey with each other. Present wireless network technology provides very incomplete tools to safeguard the wireless transition media. Confidential banking information may be escaped, lost or change in the daily transaction devices. Attackers might interrupt confidential information on the communication of mobile transmutation network through overlying and installation suitable devices of in the ectromagnetic energy, then delete, adjust, add or re-played some significant information to harm the normal use of sincere users

2.2.2 Incomplete information

In Mobil communication some time data is sanded in incomplete form Because of the process of mobile devices and variability of the communication channel, it easily leads to partial communications data. When a client using mobile phone arrive an area with poor coverage from the region with good wireless signals, or the communication is disturbed by other signals, information will occur often postponement or disappointment so communications might easily lead to unfinished data or data loss. In adding, energy shortage of mobile devices would lead the ongoing banking business to break off and make the transaction data incomplete.

2.2.3 Virus attacks

Despite the current virus on mobile operations found mainly destruct mobile phone function, consume electricity of phones and remove records of mobile phone and other information, the potential threat of mobile banking is far greater than that of the network banking. Maybe the followings can explain the reasons: firstly, the virus carried on mobile terminals can not only infect operating system of wireless network terminals but also infect that of the fixed network terminal; secondly, it is very difficult to use antivirus software for mobile devices computing power constraints; thirdly, many wireless networks don't have anti-virus measures. Recently, Russia for the first time found a computer virus, which spread via mobile networks. The virus can not only infect operating system of mobile phones with the Symbian through wireless networks, but also can spread through Bluetooth technology, that is, Mobile phones with virus will be activated, then convey a secure file including virus to near other Bluetooth-enabled mobile phones.

3 The Mobile Banking Information Security Protection Methods

From the above analysis of information safety issues of mobile banking, we can see the difference between information security issues of mobile banking and network banking. Mobile banking faces more complex security problems. We can not transplant simply security strategy of network banking to the mobile banking system, we should refer to information security of the network banking, and then introduce new technology and safety measures to protect the safety of mobile banking according to the characteristics of mobile banks. In the following part we will discuss the mobile banking protection methods.

3.1 Applying encryption technology to protect data privacy

While some security mechanism has been used in the mobile phone and wireless communications network, wireless communication arrangement such as GSM also applied encryption technology. For mobile banking application, it often includes confidential and complex information such as PIN and Bank Password, etc. The encryption technology and security mechanism of operation layer is not sufficient to protect the security of Mobile banking. Present somewhat good security encryption and authentication measures need more powerful computing power and storage volume to support. Only customers of Internet banking have a very great PC can apply the difficult encryption and authentication tools to confirm security. With low capability of operation of mobile terminal, the complex encrypted authentication technology cannot have applied to defend against security risks. In order to decrease the calculation power of the encryption and assurance the higher safety, present mobile devices start to use a symmetric encryption algorithm AES and asymmetric encryption algorithm ECC. That is , AES is a "core" and ECC "shell", The data on wireless communication is encrypted with AES, The encryption key use ECC to encrypt, This way not only safeguards that data security but also growth the speed of encryption and decryption. The AEC and the ECC are presently the most powerful encryption technology to safeguard hackers. When the hackers attack cryptograph, they need to straight attack against the AES 128. It is very difficult under the situations of the existing technology; If they select to attack the period key of ECC, they will meet the spiky problem of ECDLP. In calculation, the use of a session key is actual only for first time, so even if they get the session key, there is not much value. Temporarily, this mixture algorithm has a very small key management to reduction the volume of key management and increase its safety.

3.2 System and data integrity

For the half-finished data caused in the communication process, mobile message system should provide suitable mechanisms to avoid the incidence of non- integrity. One transporter channel, mobile stations, gateways, servers and other equipment continually face threat of malicious viruses attack and other malicious attack. Mobile banking system will be prepared with suitable security measures such as firewalls, intrusion detection system and rapid recovery mechanism to assurance data security. Integrity mechanisms of the system should be able to test integrity of system and file coding to guarantee that the integrity of mobile banking system. In the process of data communication, half-finished data communication and failure of the records should be checked constantly to find the gaps in the system.

3.3 Personality Authentication

Authentication is one of the most significant tools of defence and it is the basis of other security mechanisms in mobile banking. Presently STK is often used in Afghanistan mobile banking business such as Aziz Bank , Islamic Bank of Afghanistan , Afghan United Bank etc. Customer and the bank will sign an contract for binding between consumer identification information and phone numbers, confirmation and safety of password. The launch of customer ID information, phone numbers, password protection mechanisms require customers' authentication. The banks' access passwords are pretty simple and easy to reminisce which will basis banks' valuable information easy to extent by hackers. The characteristic of mobile devices such as movement and ease to harm make mobile banking information susceptible to attack in an open situation. South Korea and china as the world's inventor of mobile banking has been established dynamic authentication system DAS4M based on WIPI mobile podium, through casually displaying the table of characters on the screen of mobile devices, allowing to the consistent location of password on the keyboard, use corresponding figures on the keyboard to replace the password. Though such systems bring awkwardness to users, it can avoid direct attacks. Hence, we can also learn from South Korean banks and bring technology such as dynamic password and other technology currently used by the network banking to mobile banking to improve the security of mobile banking in Afghanistan banking sector.

3.4 Digital Signature

Digital Signature Technology acting an important role in the data authentication and non- repudiation. At current digital signature tools recognized by the common of people are the RSA algorithm based on the integer factorization and ECC algorithm based on elliptic bow distinct logarithm problem intended. The digital signature implanted in STK card is often applied by Afghans mobile banking application, that is, asymmetric key RSA key is entrenched in STK card, with Hash functions to get digital signature. The RSA in computing speed and security is as respectable as ECC, basically the ECC for digital signatures will be more fit for mobile banking. The aims are: firstly, ECC safety level is higher, the calculating processing speed condition is low, storage space is small, low bandwidth requisite. For RSA, more complex calculating capacity and the speed of encryption is slow.

3.5 WPKI (Wireless Public Key Infrastructure)

WPKI（Wireless Public Key Infrastructure）is progressively developed in order to meet with the needs of a wireless network authentication and encryption, this technology is presented into the wireless network area on the foundation of the Internet e-commerce PKI security method to follow a set of well-known standards for key and certificate management podium system. But WPKI is not a new standard, it uses enhanced ECC Egg-shaped curve encryption and firmness X.509 digital certificates, it also used a public key certificate management, the reliable third-party organizations----Certification Centre (CA) to prove the identity of the user, these help efficiently to create security and reliable wireless network communication area and guarantee the information safety such as data on communication, data integrity, user verification, and non-repudiation of communications. WPKI is based on the optimization of PKI. The introduction of the 100 B Elliptic Curve Crypto system in the WPKI certification decreases the storage space of Certificates. WPKI has the size limitations of the IETF PKIX certification format as well. As WPKI is a subsection of PKIX, it guarantees interoperability likelihoods among the PKI standards. WPKI accept on a public key system based on ECC algorithm and use one couple to match each other's key (encryption, decryption). When distribute a message, sender uses the public key in digital certificates of receiver to encrypt data, then receivers use its own private key to decrypt. In this way, this information can securely reach their end point. By using WPKI technology, mobile banking assurances the confidential of data, integrity, legitimacy and the identity of the non-repudiation of communications to reject the user's risk in the operation. The progress and improvement of connected technology in WPKI, the length of data and handling effort of WPKI certification will be additional summary and that achieve interoperability between WPKI and standard PKI to create well security environment for the development of mobile banks.

Conclusion

As mobile banking can offer 3A services which transcending the restriction of time and space. It will have converted popular with the development and adulthood of mobile distance communication technology as well as mobile device function better. If banks can mix the mobile banking and present services, make good use of the welfares provided by of wireless communication technology such as cell phones and develop a single customer focused on services， mobile banking will be capable to play a more significant role in banking business.

Reference

1. Schwiderski-Grosche, S, Knospe, H; Secure mobile commerce. Electronics & Communication Engineering Journal,（14：5）， 2002, pp.228 - 238
2. I. Brown, Z. ,Cajee, D. Dzvies, and S. Striebel：Cell phone banking: predictors of adoption in South Africa-an exploratory study", International Journal of Information Management, (23:5), 2003, pp.381-394
3. Hu Aiqun, Wireless Communication Network Security Issues and countermeasures. Electronic Communication Science, 2003 (12)
4. Hanafizadeh, P., Keating, B.W. and Khedmatgozar, H.R., 2014. A #systematic review of Internet banking adoption. Telematics and informatics, 31(3), pp.492-510
5. C. Odhiambo Ndalo Jowi, "Evaluation of Information Security Risk Assessment for Internet Banking Among Commercial Banks in Kenya", 2017.
6. Ula, M., Ismail, Z., & Sidek, Z. (2011). A Framework for the Governance of Information Security in Banking System. Journal of Information Assurance & Cyber Security. http://dx.doi.org/10.5171/2011.726196
7. Siddique, I., & Rehman, S. (2011). Impact of Electronic Crime in Indian Banking Sector-An Overview .International Journal of Business & Information Technology, 1(2).
8. Khan, M., & Barua, S. (2009). The Status and Threats of Information Security in the Banking Sector of Bangladesh: Polices Required. Bangladesh Journal of MIS, 1(2)
9. Paper presented " A Review on information security and banking " in information Journal for technology Research in engineering ISSN:2347-4718 , VOLUME5, ISSUE 2347-4718 APRIL , 2018